Office of the Governor
State Chief Information Officer

SECURITY

Chapter 5 – Securing Software, Peripherals and Other Equipment

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, “State Information Technology Services.”

Statutory Authority: G.S. §147-110

Section 01 Purchasing and Installing Hardware

050101 Specifying Information Security Requirements for New Hardware

Purpose: To ensure that security requirements are a part of the hardware acquisition process.

STANDARD

Agencies shall ensure that new hardware purchases are supported by documented operational, technical and security requirements.

Prior to hardware purchase, the agency shall formally document, at a minimum, how the new hardware acquisition meets the following evaluation criterion:

- Proposed vendor hardware design complies with information security and other State policies and standard security and technical specifications, such as the following:
  - □ The vendor has configured the system with adequate capacity to fulfill the functional requirements stated in the agency’s design document.
  - □ The vendor has configured hardware security controls to adequately protect data. (Optionally, the vendor may assist the agency with the configuration of software security controls to provide adequate data protection on the vendor’s hardware.)
  - □ The vendor shall provide system availability data to demonstrate that the proposed hardware meets minimum downtime requirements.

ISO 17799: 2005 References
12.1.1 Security requirements analysis and specification

050102 Specifying Detailed Functional Needs for New Hardware

Purpose: To ensure that functional requirements are part of the acquisition process.

STANDARD

Agencies shall follow State procurement policies when acquiring hardware to ensure that the purchase meets specified functional needs. Agencies shall include specific requirements for performance, reliability, cost, capacity, security, support and compatibility in Requests for Proposals (RFPs) to properly evaluate quotes.

GUIDELINES

Agencies should develop a process to define hardware functionality prior to purchasing.

Other requirements to consider and include in RFPs are the following:

- If hardware will support a critical function: replacement availability and times.
- If hardware will be used outside of a permanent facility (such as mobile equipment): requirements for survivability (i.e., extreme conditions such as temperature, dust, humidity, etc.)
- If data confidentiality, criticality and integrity needs dictate: hardware-based encryption or other applicable security requirements.

ISO 17799: 2005 References
12.1.1 Security requirements analysis and specification

050103 Installing New Hardware

Purpose: To ensure that new hardware is subjected to operational and security review prior to installation.

STANDARD

Agencies involved with the installation of new hardware shall establish a formal review process that allows entities affected by the new hardware to review and comment on the implementation plans and the operational and security requirements.

The review process shall include, but not be limited to, the following:

- Notification of all impacted parties prior to the installation of new hardware.
- Circulation to appropriate individuals of planned changes or disruptions to operational status or information security for the new installation.
- Installation of equipment in an appropriately secured and environmentally controlled environment.

- Restricting access to the proposed changes (i.e., network diagrams, security features, locations, configurations, etc.) to those who require the information to perform their job duties.
- Performing a risk analysis on the hardware installation process, including possible worst-case scenarios.

ISO 17799: 2005 References
12.1.1 Security requirements analysis and specification

050104 Testing Systems and Equipment

Purpose: To require that new systems and equipment undergo user acceptance testing before being placed into a production environment.

STANDARD

Agencies shall develop a process to ensure that new systems and equipment are fully tested against operational and security requirements and formally accepted by users before management accepts the systems and places equipment into the operational environment.

GUIDELINES

Full and comprehensive testing of systems and equipment should entail following a written test plan that includes, but is not limited to, the following:

- Approval from the manager responsible for the correct functioning of the information system to ensure that all relevant security policies and requirements are met and the system provides an acceptable level of risk.
- Assessment of compatibility with other system components.
- Determination that technical and functional specifications are met.
- Beta testing from cross-sections of users in different departments of the agency.

ISO 17799: 2005 References
12.1.1 Security requirements analysis and specification

Section 02 Cabling, UPS, Printers and Modems

050201 Supplying Continuous Power to Critical Equipment

Purpose: To minimize the risks of critical equipment downtime and data loss caused by power outages or electrical anomalies.

STANDARD

Agencies shall protect critical information technology systems from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems continue to perform during power outages and electrical anomalies (e.g., brownouts and power spikes).

GUIDELINES

The three primary methods for providing continuous power are:

- Multiple electric feeds to avoid a single point of failure in the power supply.
- Backup generator(s).
- Uninterruptible power supply (UPS).

Each agency should examine the availability requirements for critical equipment and determine which combination of these three methods best meets the needs of the agency. Most scenarios will require at least two of the techniques.

When analyzing the power requirements of critical systems, agencies should consider the following best practices:

- Both power and communication lines should be protected.
- Multiple power feeds should not enter a building in proximity to each other.
- Using a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges. Because most UPS batteries do not last for more than four (4) hours without a continuous supply of power, the following actions should be taken.
  - ❑ Development of contingency plans that include procedures to follow if the UPS fails.
  - ❑ Inspections of UPS equipment to ensure that the equipment:
    - Has the ability to sustain, for a predefined period, the power load of the systems and equipment it supports.
    - Is serviced according to the manufacturer’s specifications.
- A backup generator should be used when requirements demand continuous processing in the event of a prolonged power failure. Agencies that require a backup generator should ensure that:
  - ❑ The generator is serviced regularly in accordance with the manufacturer’s specifications.
  - ❑ An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period.

Other practices that help mitigate the risk of power outages include:

- Locating emergency power switches near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency.
- Providing emergency lighting in case of a main power failure.
- Installing lightning protection in all buildings.
- Fitting all external communications lines with lightning protection filters.
- Utilizing alternate fuel sources such as:

- ❑ Solar energy
- ❑ Fuel cell electricity
- ❑ Biogas
- ❑ Geothermal electricity

ISO 17799: 2005 References
9.2.2 Supporting utilities

050202 Managing and Maintaining Backup Power Generators

Purpose: To ensure continuity of backup power during power outages.

STANDARD

Agencies with business requirements that demand uninterrupted information processing during power outages shall deploy backup power generators. When a backup generator is employed, agencies shall:

- Regularly inspect the generator to ensure that it:
  - ❑ Remains compliant with both safety and manufacturer maintenance requirements.
  - ❑ Has an adequate supply of fuel.
- Ensure that the generator:
  - ❑ Has the capacity to sustain the power load required by supported equipment for a prolonged period of time.
- Is tested regularly according to the manufacturer’s specifications but no less than quarterly.

GUIDELINES

- Backup generators are usually combined with an uninterruptible power supply to protect critical information technology systems that demand high availability. Such a combination both supports an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss, and can also provide continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption.
- Contingency plans should include procedures to be followed in the event the backup generator fails.

ISO 17799: 2005 References
9.2.2 Supporting utilities

050203 Using Fax Machines/Fax Modems

Purpose: To protect confidential information transmitted via facsimile machines or facsimile modems.

STANDARD

Agencies may transmit confidential information using facsimile machines or facsimile modems only when security is in place to protect the information being sent.

Where receiving facsimile machines are in open areas, personnel using facsimiles to transmit confidential information shall notify the intended recipient when the information is being sent and the number of pages to expect, so that facsimiles containing confidential information are not left unattended on a facsimile machine.

GUIDELINES

Agencies should implement formal procedures that require both the sender of the information and the intended recipient to authorize the facsimile transmission /and recipient facsimile phone number before the transmission occurs/ and to verify successful transmission upon receipt.

Agencies should incorporate reminders and education about the security issues that surround the use of facsimile machines and facsimile modems into their ongoing information security training and awareness programs.

RELATED INFORMATION

Standard 030404	Receiving Misdirected Information by Facsimile
Standard 030408	Receiving Unsolicited Facsimiles

ISO 17799: 2005 References
10.8.5 Business information systems

050204 Using Modems/ISDN/DSL Connections

Purpose: To protect confidential information being transmitted over public networks.

STANDARD

Agencies using modem (cable or telephone)/ISDN/DSL connections to transmit confidential information over public networks shall implement the following security measures to prevent disclosure of the confidential information:

- The agency shall require personnel to encrypt or transmit through a secure connection such as VPN or SSL all confidential information, including user passwords and Social Security numbers, to protect the confidentiality and integrity of the information.
- The agency shall require those who transmit information via these types of connections to notify the intended recipient that the information is being sent.

ISO 17799: 2005 References
10.8.5 Business information systems

050205 Using Centralized, Networked or Stand-Alone Printers

Purpose: To prevent the release of confidential information to unauthorized persons via printers.

STANDARD

Personnel shall transmit confidential information to printers residing in common areas only when there is a person authorized to receive the information present to protect the confidentiality of the material coming off the printer.

RELATED INFORMATION

Standard 030702	Photocopying Confidential Information
Standard 030811	Printing Classified Documents

ISO 17799: 2005 References

10.7	Media handling
11.3.3	Clear desk and clear screen policy

050206 Installing and Maintaining Network Cabling

Purpose: To ensure the availability and integrity of data by protecting network cabling.

STANDARD

In addition to complying with the NC Electrical Code[1], agencies that install and/or maintain network cabling shall use only qualified personnel to perform tasks involving this cabling. Agencies shall implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling.

GUIDELINES

Agencies installing or maintaining network cabling should consider the following practices to increase the security and physical protection of cabling where appropriate:

- Using underground cabling, where possible, or providing lines with adequate alternative protection.
- Running network cabling through overhead cable troughs, pipes or similar conduits.
- Limiting the amount of exposed cabling within public areas.
- Eliminating interference by segregating power cables from communications cables.
- Installing fiber-optic cabling.

[1] Chapter 8, Article 830 of the code addresses “Network Powered Broadband Systems”. Other provisions apply as well.

ISO 17799: 2005 References

9.2.3	Cabling security

Section 03 Consumables

050301 Controlling IT Consumables

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References

10.7.1	Management of removable media

050302 Using Removable Storage Media, Including Diskettes and CDs

Purpose: To protect the State's data contained on removable storage media from unauthorized disclosure and modification.

STANDARD

Security controls shall be put in place to protect the confidentiality and integrity of data contained on removable storage media throughout the life of those storage media, including disposal. Access controls shall include physical protection of and accountability for removable media to minimize the risk of the following:

- Damage to data stored on the removable storage media.
- Theft.
- Unauthorized access of data stored on the media.
- Software licensing violations.

GUIDELINES

Authorized data users may use removable media to transfer information to another authorized data user in compliance with all applicable policies, regulations and laws.

RELATED INFORMATION

Standard 030505	Receiving Information on Disks
Standard 030604	Archiving Information
Standard 050302S	Standards for Clearing or Destroying Media

ISO 17799: 2005 References

10.7	Media handling

Section 04 Working Off Premises or Using Outsourced Processing

050401 Contracting or Using Outsourced Processing

Purpose: To ensure that outsourced processing achieves acceptable service levels.

STANDARD

Agencies that outsource their information processing must ensure that the service provider demonstrates compliance with industry quality standards.

Outsourcing agreements shall include a service level agreement (SLA) that, at a minimum, meets State information technology security requirements.

Outsourcing agreements shall include:

- The agency's course of action and remedy if the vendor's security controls are inadequate such that the confidentiality, integrity or availability of the agency's data cannot be assured.
- The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters.
- The vendor's ability to provide processing in the event of failure(s).

ISO 17799: 2005 References

6.2.1	Identification of risks related to external parties
12.5.5	Outsourced software development

050402 Issuing Laptop/Portable Computers to Personnel

Purpose: To protect confidential data on laptop/portable computers and other handheld computing devices.

STANDARD

Agencies shall authorize the assignment of portable personal computers to employees and require that users comply with all information technology security policies when using the portable devices, including the agency and statewide acceptable use policies, as applicable. Portable devices covered by this standard are those that connect to agency and State networks and/or store agency data and include:

- Handheld devices (electronic organizers, personal digital assistants [PDAs], Pocket PCs, etc.).
- Smart phones, cellular phones and pagers.
- Flash drives and thumb drives.

GUIDELINES

- Agencies' management should consider using the following additional security controls, as appropriate:

- ❑ Check-in procedures for portable devices that verify that the device is free of unauthorized software, viruses, or any other malicious code prior to reissue or reconnection to the network.
- ❑ Training to raise user awareness of the additional risks that accompany mobile computing and the controls with which users must comply.

RELATED INFORMATION

Standard 050403	Using Laptop/Portable Computers

ISO 17799: 2005 References
11.7.1 Mobile computing and communications

050403 Using Laptop/Portable Computers

Purpose: To promote the secure use of laptops and other portable devices.

STANDARD

Agencies shall implement appropriate safeguards to ensure the security of laptops and other portable computing devices. Specifically:

- Portable computing devices shall:
  - ❑ Be physically secured when the users have taken them out of a secure area.
  - ❑ Be labeled with tamper-resistant tags identifying the device as property of the State, a permanently engraved serial number or both.
  - ❑ Comply with all applicable security requirements for desktops.
- The BIOS password on such devices, if applicable, must be enabled.
- When a laptop is outside a secure area, data on the laptop must be backed up, and the backup must be kept separate from the laptop.

GUIDELINES

The small size and mobility of portable computing devices are the primary causes of the attendant security risks. Information security controls that agencies should consider include, but are not limited to, the following:

- Procedures governing appropriate use of portable devices in unprotected areas (meeting rooms and off-site locations).
- Restricting use of such devices via a wireless connection that originates from anywhere other than State- or agency-approved networks.
- Training on how to physically secure devices against theft when left in cars or other forms of transport, hotel rooms, conference centers and meeting places.

- Training to raise user awareness of the additional risks that accompany mobile computing and the controls that should be implemented.

ISO 17799: 2005 References

9.2.5	Security of equipment off-premises
11.7.1	Mobile computing and communications

050404 Working from Home or Other Off-Site Location (Teleworking)

Purpose: To secure and protect communications with agency information resources while personnel are working at off-site locations.

STANDARD

Personnel shall not work from home or off site using State-issued or personally owned computers or devices (commonly known as teleworking or telecommuting) unless authorized by agency management. Agencies that authorize teleworking for their personnel shall ensure the following:

- Agencies shall define standards for authorized personnel to securely access systems from off site. Standards shall include:
  - ❑ Use of agency-approved virus prevention and detection software.
  - ❑ Use of personal firewalls.
  - ❑ Securing home wireless networks.
  - ❑ Protecting portable electronic devices such as personal digital assistants (PDAs) and smart cell phones (combination PDA/cell phone/camera phones).
  - ❑ Use of virtual private networking software or other technologies for protecting communications between off-site systems and agency information resources.
  - ❑ Use of two-factor authentication products (such as one-time password tokens or biometric devices) to authenticate users, if applicable.
  - ❑ Use of encryption products to protect data stored on off-site systems, if applicable.
- Agencies shall provide training to personnel for properly accessing systems from off site and for keeping antivirus software and personal firewall software up to date with the latest signature files and patches.
- Agencies shall also provide instructions and training for protecting confidential information transferred to, processed on or stored on non-State-issued systems, such as personal computers at home.
- Agencies shall document and retain evidence of training provided to a user during the time that the individual is authorized to access systems remotely.

Agency employees who are authorized to work from home shall ensure that the agency-defined standards for off-site work are strictly adhered to. Personnel shall take extra precautions to ensure that confidential information stored on personal computers or electronic devices is not divulged to unauthorized persons, including family members.

RELATED INFORMATION

Standard 020112	Controlling Remote User Access
Standard 050408	Day-to-Day Use of Laptop/Portable Computers

ISO 17799: 2005 References

9.2.5	Security of equipment off-premises
11.7.2	Teleworking

050405 Moving Hardware from One Location to Another

Purpose: To protect hardware during moves.

STANDARD

To protect agency hardware and the data residing on the hardware, only authorized, trained personnel shall be allowed to move hardware from one location to another.

GUIDELINES

Agencies should consider the following information security issues when moving hardware:

- The confidentiality and integrity of data can be compromised if unauthorized persons gain possession of the hardware.
- Equipment can be damaged if handled improperly.

ISO 17799: 2005 References

9.2	Equipment security

050406 Using Mobile Phones

Purpose: To protect confidential information during mobile phone use.

STANDARD

Personnel using mobile phones shall refrain from discussing topics considered confidential by the agency. The amount of personal conversations on agency-provided mobile phones shall be controlled in accordance to the agency's acceptable use policy.

GUIDELINES

Agencies that issue mobile phones to personnel should make them aware of the following information security issues:

- The risk of others' eavesdropping in both private and public areas.
- The risk involved in storing confidential information on calendars, address books, etc.
- Their responsibility for the safekeeping of assigned phones.

ISO 17799: 2005 References
9.2.5 Security of equipment off-premises
10.8.5 Business information systems

050407 Using Business Center Facilities

Purpose: To establish appropriate use requirements when information is processed in external business centers or facilities.

STANDARD

Agency employees using external business centers to conduct business shall not process confidential information, including not transmitting confidential information via email(s) or fax(es).

When agency employees use business center facilities for processing other government information (i.e., information that is not confidential), they shall:

- Refrain from using auto-save features on the facility's equipment and delete, prior to leaving the facility, any files that were temporarily saved to the hard disk of the equipment they were using.
- Clear history and cache memory and delete cookies prior to leaving the facility.
- Never leave the computer on which they are working unattended.
- Clear the facility's printer(s) of all documents they have printed.

ISO 17799: 2005 References
11.7.1 Mobile computing and communications

050408 Day-to-Day Use of Laptop/Portable Computers

Purpose: To promote the secure day-to-day use of laptop/portable computers.

STANDARD

Personnel who use an agency laptop/portable computer shall ensure that the laptop/portable computer and the information it contains are suitably protected at all times.

Where appropriate, agencies shall require that laptops and other State-issued mobile electronic devices have:

- Locks.

- BIOS password protection.
- Cryptographic capabilities for confidential information.
- Regular backups.
- Current antivirus software.
- Firewalls configured to comply with State and agency policies.

Agencies shall periodically audit these devices to ensure compliance with these requirements.

ISO 17799: 2005 References
11.7.1 Mobile computing and communications

Section 05 Using Secure Storage

050501 Using Lockable Storage Cupboards

Purpose: To secure valuable material or equipment within lockable cupboards.

STANDARD

Agencies shall store valuable equipment and confidential information securely, according to its classification status.

Where appropriate, agencies shall store resources in lockable storage cupboards where the physical security controls are sufficient to protect the equipment from theft.

RELATED INFORMATION

Standard 090101	Preparing Premises to Site Computers
Standard 090102	Securing Physical Protection of Computer Premises
Standard 090103	Ensuring Suitable Environmental Conditions
Standard 090104	Physical Access Control to Secure Areas

ISO 17799: 2005 References
9.1.3 Securing offices, room and facilities

050502 Using Lockable Filing Cabinets

Purpose: To secure paper-based files and computer media in locked filing cabinets.

STANDARD

Agencies shall use lockable file cabinets to store confidential information such as paper documents and computer media in a manner that is commensurate with the classification status of the information.

RELATED INFORMATION

Standard 090101	Preparing Premises to Site Computers
Standard 090102	Securing Physical Protection of Computer Premises
Standard 090103	Ensuring Suitable Environmental Conditions
Standard 090104	Physical Access Control to Secure Areas

ISO 17799: 2005 References
9.1.3 Securing offices, rooms and facilities

050503 Using Fire-Protected Storage Cabinets

Purpose: To decrease the risk of critical information being destroyed by fire.

STANDARD

Where appropriate, agencies shall provide fire-protected storage for documents and media containing information critical to their business function:

GUIDELINES

Agencies should consider the following physical security issues:

- Securing critical information in a fire-resistant safe or cabinet should be part of an agency's clear desk policy.
- Regardless of the rated capacity of a fire-resistant container, events surrounding a fire (heat, smoke, water, chemicals) may render any information that is stored in the container unusable; therefore, off-site backups of critical information remain essential.

ISO 17799: 2005 References
9.1.3 Securing offices, rooms and facilities
11.3.3 Clear desk and clear screen policy

050504 Using a Safe

Purpose: To protect critical information from theft, destruction and misuse

STANDARD

Where appropriate, agencies shall store information that is confidential or critical to their business functions in a safe.

When a safe is used:

- The location of the safe shall be inconspicuous, so as not to draw additional attention to the physical security of the safe.
- The location of the safe must have a load-bearing capacity sufficient to support the weight of the safe.

- The location of the safe must be in an area that is subject to regular surveillance.
- Access to the safe shall be limited to those who agency management has determined require access to perform their job duties.

GUIDELINES

Whenever the value of confidential or critical paper-based files or computer media warrants the use of a safe, agencies should consider the following:

- Critical information is compromised if the whole safe is stolen.
- Events surrounding a fire (heat, smoke, water, chemicals) may render the material stored in the safe unusable; therefore, off-site backups of critical information remain essential.

RELATED INFORMATION

Because the security of the safe itself is also critical, agencies should review information on physical security in Chapter 9, Section 1, Premises Security.

ISO 17799: 2005 References

9.1.3	Securing offices, rooms and facilities
11.3.3	Clear desk and clear screen policy

Section 06 Documenting Hardware

050601 Managing and Using Hardware Documentation

Purpose: To effectively manage hardware assets and their documentation.

STANDARD

Agencies shall retain user documentation and technical specifications of information technology hardware. Documentation shall be secured from unauthorized use and made readily available to support system maintenance and system support staff.

GUIDELINES

Agencies should develop and maintain additional documentation that details hardware placement and configuration, provides flowcharts, etc. Issues to be considered with document management include, but are not limited to, the following:

- Negligence in performing recommended scheduled maintenance could jeopardize business operations.

ISO 17799: 2005 References

7.1.1	Inventory of assets
10.7.4	Security of system documentation

050602 Maintaining a Hardware Inventory or Register

Purpose: To maintain accountability for hardware assets and protect them from misappropriation.

STANDARD

Each agency shall identify and record its information technology (IT) hardware assets in a formal hardware inventory/register. Each agency shall develop a process to ensure that IT hardware is identified with agency-unique physical asset tags and that the inventory/register is kept up to date. The formal hardware inventory/register should include only information that is available for public inspection.

ISO 17799: 2005 References
7.1.1 Inventory of assets

Section 07 Other Hardware Issues

050701 Disposing of Obsolete Equipment

Purpose: To protect data confidentiality and integrity through proper disposal of obsolete equipment.

STANDARD

Agencies shall establish a procedure for certifying that data have been properly removed from information technology equipment before it is transferred, surplused or donated.

The data contained on information technology equipment must be permanently removed by destroying, degaussing, or using a wipeout utility. The utility must be approved by the National Institute of Standards and Technology (NIST)[2] or comply with approved Department of Defense standards so that previously recorded information is not recoverable. The method of data removal shall be based on what is reasonable and practical.

ISO 17799: 2005 References
9.2.6 Secure disposal or re-use of equipment

050702 Recording and Reporting Hardware Faults

Purpose: To maximize hardware availability and integrity through fault recording/reporting.

[2] NIST documents addressing data removal software can be found at http://csrc.nist.gov/fasp/FASPDocs/disksanitizebsp.htm and http://csrc.nist.gov/fasp/FASPDocs/inoutput-control/NIHDataSanBSP.htm.

STANDARD

Users who identify a hardware fault or information-system-processing problem shall promptly report the problem and the details to the appropriate support staff.

Each agency shall establish procedures to record and track equipment faults.

RELATED INFORMATION

Standard 130402 Analyzing Information Security Incidents Resulting from System Failures

Incident Response Standard

ISO 17799: 2005 References

9.2.4	Equipment maintenance
10.10.5	Fault logging

050703 Insuring Hardware

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References

9.2.4	Equipment maintenance
9.2.5	Security of equipment off-premises

050704 Insuring Laptops/Portables for Use Domestically or Abroad

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References

9.2.4	Equipment maintenance
9.2.5	Security of equipment off-premises

050705 Clear Screen

Purpose: To protect confidential information from unauthorized disclosure.

STANDARD

To protect confidential data from disclosure, desktops and laptops shall have an agency-approved screen saver with a screen lock that engages after the keyboard and/or the mouse have been idle for a period of thirty (30) minutes or less.

RELATED INFORMATION

Standard 30902 Loading Personal Screen Savers

ISO 17799: 2005 References

9.1	Secure areas
11.3.3	Clear desk and clear screen policy

050706 Logon and Logoff from your Computer

Purpose: To make individual access security controls more effective

STANDARD

All computer users shall have a unique user ID and a password known only to themselves to log on to and/or access their information resources.

Users must adhere to approved login and logoff procedures by:

- Creating strong passwords and managing them appropriately.
- Minimizing the opportunity for others to learn their passwords.

When not in use for an extended period of time, each desktop/laptop shall be turned off, except as specifically authorized by the agency security administrator.

RELATED INFORMATION

Standard 020106	Managing Passwords
Standard 100302	Keeping Passwords/PINs Confidential

ISO 17799: 2005 References

11.2	User management
11.3.3	Clear desk and clear screen policy

050707 Dealing with Answering Machines/Voice Mail

Purpose: To prevent confidential information from being disclosed in messages left on telephone answering machines and voice mail.

STANDARD

Users shall not record or leave messages containing confidential information on answering machines or voice mail systems.

GUIDELINES

Agencies should communicate in their training for personnel that confidential information is not to be left on answering machines or voice mail systems.

RELATED INFORMATION

Standard 030403	Recording of Telephone Conversations
Standard 030406	Giving Instructions over the Telephone
Standard 050406	User Logon and Logoff from Computers

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

050707 Taking Equipment off the Premises

Purpose: To safeguard and maintain accountability for equipment.

STANDARD

Agency personnel must have approval from an authorized agency employee before they remove State information technology equipment from agency facilities. Personnel removing equipment shall be responsible for the security of the equipment at all times.

Agencies shall establish procedures for the removal and return of agency equipment. Where appropriate, logging procedures shall be established to track the removal (sign-out) of equipment from and return (sign-in) of equipment to the agency.

ISO 17799: 2005 References
9.2.5 Security of equipment off-premises
9.2.7 Removal of property

050709 Maintaining Hardware (On-Site or Off-Site Support)

Purpose: To maintain hardware availability and integrity.

STANDARD

Each agency shall provide or arrange maintenance support for all equipment that is owned, leased or licensed by the agency. The agency must arrange support services through appropriate maintenance agreements or with qualified technical support staff. When maintenance support is provided by a third party, nondisclosure statements shall be signed by authorized representatives of the third party before any maintenance support is performed. Records of all maintenance activities shall be maintained.

ISO 17799: 2005 References
9.2.4 Equipment maintenance

050710 Using Speed-Dialing Telephone Options

Purpose: To protect information stored in telephone system equipment.

STANDARD

Agencies shall incorporate security measures to protect confidential information, such as unlisted telephone numbers, stored in speed-dialing systems.

GUIDELINES

Agencies should consider the information security issues and the accompanying risks involved if unlisted phone numbers are acquired by unauthorized users.

ISO 17799: 2005 References

10.8.1	Information exchange policies and procedures

050711 Cleaning of Keyboards and Screens

Purpose: To maintain equipment availability through safe and appropriate cleaning.

STANDARD

To prevent damage to equipment and loss of data, agencies shall provide only safe and approved cleaning materials to personnel for the cleaning of their keyboards and screens.

ISO 17799: 2005 References

9.2.4	Equipment maintenance

050712 Damage to Equipment

Purpose: To improve confidentiality, integrity and availability of data by requiring the reporting of property damage.

STANDARD

Each user shall report deliberate or accidental damage to agency equipment or property to his or her manager as soon as it is noticed.

GUIDELINES

Damage to equipment or property that performs a security function may create a weak link in the agency’s security architecture and leave confidential information exposed. Agencies should refer to their business impact analyses and/or risk analyses to determine the level of urgency in repairing or replacing damaged equipment.

ISO 17799: 2005 References

9.2.4	Equipment maintenance
10.10.5	Fault logging

HISTORY

State CIO Approval: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
Identification and Authentication Using IDs and Passwords	050706 – Logon and Logoff from your Computer 020106 – Managing Passwords 100302 – Keeping Passwords/PIN Numbers Confidential
Remote Access Policy, including Mobile Computing and Telecommuting	050404 – Working from Home or Other Off-Site Location (Teleworking) 020112 – Controlling Remote User Access 030103 – Accessing Your Network Remotely
User ID and Password	050403 – Using Laptop/Portable Computers 020106 – Managing Passwords 100302 – Keeping Passwords/PIN Numbers Confidential
Permanent Removal of Data from Electronic Media Standard	050701 – Disposing of Obsolete Equipment 030903 – Using External Disposal Firms 040301 – Disposing of Software
Desktop and Laptop Security Standard	050402 – Issuing Laptop/Portable Computers to Personnel 050403 – Using Laptop/Portable Computers 050408 –Day to Day Use of Laptop/Portable Computers 050705 – Clear Screen 050706 – Logon and Logoff from your Computer 020103 – Security Unattended Work Stations 020106 – Managing Passwords 030902 – Loading Personal Screensavers